UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/813,358	03/31/2004	Alan Frank Graves	14658	5013

293 7590 08/23/2007

Ralph A. Dowell of DOWELL & DOWELL P.C.
2111 Eisenhower Ave
Suite 406
Alexandria, VA 22314

EXAMINER	
POLTORAK, PIOTR	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
08/23/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/813,358	GRAVES ET AL.	
	Examiner	Art Unit	
	Peter Poltorak	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 March 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-60* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22, 34-52* is/are rejected.

7)☒ Claim(s) *23-33 and 53-55* is/are objected to.

8)☒ Claim(s) *56-60* are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *9/03/04, 8/24/06, 2/27/07*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. In response to restriction mailed out on 5/18/07 applicant elected Invention I (claims 1-55) with traverse.

2. Although applicant fails to provide justification for applicant's opinion that "the Examiner has failed to establish that a search of the complete application would be an undue burden", the examiner reiterates that Invention (I) is directed towards a method and a system comprising preserving confidentiality of sensitive information stored in memory, classified in class 713, subclass 193 would not require search for selecting operating code for use by the end user device on the basis of the operational characteristics of the end user device or transmitting an operating system code to the end user device to enable the end user device to transmit a message requesting authentication of a user, while invention (II) classified in class 726, subclass 2, is directed toward an apparatus selecting operating code for use by the end user device on the basis of the operational characteristics of the end user device and to transmitting to the end user device operating system code to enable continued use of the end user device by the user, and would not require a search for determining whether confidentiality of the sensitive information stored in the memory store is to be preserved or an encryption module communicatively coupled to a control entity and a data bus encrypting data in accordance with an encryption key.

3. Claims 1-55 have been examined.

Claim Objections

4. The phrase "sending a message ... instrumental in causing the end user device ..." is not clear, since the term "instrumental" is a subjective term that is open to various interpretation. For purpose of the further examination the phrase is treated as "sending a message ... causing the end user device ...".
5. In claims 37 and 49 the following lack antecedent basis:
    a. Claim 37: "the user interface" (in light of claim 16, the claim is treated as directed towards "a user interface"),
    b. Claim 49: "the server" and "the memory store",
6. The phrase: "...detecting an identification code of a potential user proximate the end user device..." in claim 24 appears to be missing "to".
7. Claim 50 misses a comma at the end of the limitation. Furthermore, the claim 50 consists of the limitation: "wherein the sensitive information comprises healthcare information". It is not clear how the limitation specifying the information to be healthcare information, limits claim 49. Claim 50 neither provides any particular distinction of healthcare information from other type of information nor it includes any additional limitation which would employ the specific healthcare information (these information are essential no functional objects), and it is not clear how simply using a particular name or directing the method to a particular type of information (e.g. healthcare information) would affect (further limit) the steps of the method disclosed by claim 49.
8. Claims 3, 6-8, 10-12 14-16 and 25-33 are rejected by virtue of their dependence.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

9. Claims 52 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

10. The specification provides no guidance in teaching how the limitations of claim 52, which incorporate the limitation of claim 51, could be accomplished. The claim language is addressed towards a session between an application server and an end user device upon which responsive to the detecting of a requirement to preserve confidentiality ... a message is sent to the end user device. Claim 52 limits the detecting of the requirement comprising detecting termination of the session at the application server. It is not clear how the end user device receives the message after the session is terminated.

> *51. A method, comprising: - establishing a healthcare session with an end user device servicing an authenticated user; providing sensitive healthcare information to the end user device for storage thereon during the healthcare session; detecting existence of a requirement to preserve confidentiality of the sensitive healthcare information; responsive to the detecting, sending a*

message to the end user device instrumental in causing the end user device to preserve the confidentiality of the sensitive healthcare information.

52. The method defined in claim 51, the healthcare session being established between the end user device and an application server, wherein detecting existence of a requirement to preserve confidentiality of the sensitive healthcare information comprises detecting ***termination of the session at the application server****.*

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

11. Claims 7 and 52 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter that applicant regards as the invention.

12. It is not clear whether the limitation of claim 7 insists that "a host" providing "stimuli" differ from "a host" providing instruction recited in claim 6 or whether inappropriate term is used, which would make sense in light of the specification and the claim language. For purpose of the further examination the examiner considers "a host" in claim 7 to read "the host".

13. The limitations of claim 52 are not understood. It appears that some essential steps are not disclosed in the claim language because the claim language suggests that a (end user) device preserves confidentiality when it receives a message. However, the message is to be received after the session with the device is terminated.

51. A method, comprising: - establishing a healthcare session with an end user device servicing an authenticated user; providing sensitive healthcare information to the end user device for

storage thereon during the healthcare session; detecting existence of a requirement to preserve confidentiality of the sensitive healthcare information; responsive to the detecting, sending a message to the end user device instrumental in causing the end user device to preserve the confidentiality of the sensitive healthcare information.

52. The method defined in claim 51, the healthcare session being established between the end user device and an application server, wherein detecting existence of a requirement to preserve confidentiality of the sensitive healthcare information comprises detecting ***termination of the session at the application server****.*

Appropriate correction is required.

Claim Rejections - 35 USC § 102 or 103

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claims 15-22, 34, 36-37, 49-50 are rejected under 35 U.S.C. 102(b) as anticipated by or, in the alternative, under 35 U.S.C. 103(a) as obvious over Windows NT/2000 as illustrated by Schmidt (Jeff Schmidt, "Microsoft Windows 2000 Security Handbook", ISBN: 0789719991, August 2000).

As per claims 15-22, 34, 49 Schmidt teaches Window NT/2000 network environment implementing an end user device communicating with a server (e.g. Fig. 13.1, pg. 268). Schmidt discloses server supporting for authenticated users (e.g. "Authentication", pg. 277), and discloses that the system supports TCP/IP communication (pg. 147). In TCP/IP each communicating entity manages a communication session (e.g. "Large Window Support", pg. 147). Furthermore, an ordinary artisan would recognize that computers utilizing Windows NT/2000 comprise a memory store (e.g. hard disks) and are operative to store sensitive information (e.g. SAM database, pg. 318) during the session.

15. Schmidt discloses that end user device determine whether confidentiality of the sensitive information stored in the memory store is to be preserved and responsive to determining the confidentiality of the sensitive information stored in the memory store is to be preserved, taking an action to preserve confidentiality of the sensitive information stored in the memory store based on stimuli received via the user interface and the network interface ("The General Logon Sequence" and "Authentication Procedure", pg. 320-322, and "Account Lockout Policy", pg. 560, for example. Note that Windows provides at least two types of procedures that read on the claim language. In addition to prevent a user to access confidential information when input password and user name do not are not correct Windows protects confidential information responsive to Control-Alt-Delete command, see USPN 5664099 referring to Windows NT, for example).

16. The examiner considers Microsoft 2000, Kernel to read on the control entity.

17. As per claim 34, only a proper authentication allows a user to pass the log-in module and access the memory store.

18. As per claim 36, Schmidt discloses Microsoft 2000's Encrypted File System (EFS, 210 and 470-471).

19. As per claims 37, Microsoft 2000 locking an account suggested by Schmidt on pg. 560 would result in disabling a user interface.

20. As per claim 50, Schmidt does not disclose that the sensitive information comprises healthcare information. However, the examiner points out that implementing Schmidt's invention into various type of information (e.g. healthcare information) would not affect the functionality of the invention. Additionally, the Official Notice is taken that it is old and well known to store sensitive information that is healthcare information in a memory store (e.g. medical records stored on PCs and/or Servers, e.g. USPub. 2002/0026105, USPub. 2003/0179223, USPub. 2003/0208382 etc.), and it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement Microsoft 2000 invention as disclosed by Schmidt into healthcare information given the benefit of security.

21. Claims 15-16, 35-36, 44-51 are rejected under 35 U.S.C. 102(b) as anticipated by or, in the alternative, under 35 U.S.C. 103(a) as obvious over Windows 2000 as illustrated by Microsoft TechNet" (Microsoft TechnNet "Data Protection Implementing the Encrypting File System in Windows 2000" posted in "Windows 2000 File Systems Tutorials", in particular: "Step-by-Step Guide to Encrypting File System (EFS)" article on 05/2002).

As per claims 15-16, 49-50, Microsoft TechNet discloses encrypting a file or folders by Windows 2000 ("Encrypting a file or folder"). End user devices implementing Windows 2000 are implemented on computers and computers comprise processor and memory. The process of encrypting files or folders evidences the presence of a memory store operative to store sensitive information during the session. Windows 2000 discloses that determining whether confidentiality of the sensitive information stored in the memory store is to be preserved and responsive to determining that confidentiality of the sensitive information store in the memory store is to be preserved, taking an action to preserver confidentiality of the sensitive information stored in the memory store (see "Encrypt contents to secure data selection" in "Encrypting a file or folder" section).

The "Folder and File Encryption On a Remote Server) provides evidence of a control entity operative to support a session with the server for an authenticated user.

22. The decryption process disclosed in "Decrypting Files and Folders" section reads on claim 44 and as per claim 45, Windows 2000 discloses that in order to provide encryption an authorized administrator must enable encryption ("Encrypting a file or folder" section) and an ordinary artisan would readily recognize that in addition to a user interface enabling encryption in order to encrypt files on a remote server (as disclosed in "Folder and File Encryption On a Remote Server" section) requires a network interface.

23. As per claim 36, encryption reads on data scrambling.

24. As per claim 35, an ordinary artisan would readily recognize that encryption would replace the unencrypted information and, as a result, the sensitive (unencrypted information) would be erased.

25. As per claim 47, although Windows 2000 does not disclose that the end user device is a mobile wireless device, an Official Notice is taken that it is old and well known in the art of computing to use mobile wireless devices (e.g. laptops in wireless Ethernet environment), and it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement Windows 2000 invention in an end user device that is a mobile wireless device given the benefit of portability.

26. As per claim 48, a wireless interface/card provides information regarding the interface (e.g. 802.11 standard connection), which would read on a label, and since each interface has different maximum distance from a receiver the examiner treats the label broadly as indicative of an inability to function outside a predetermined location.

    Also, the examiner points out that any distance outside of a predetermined network location result in no network connection and mobile devices frequently disclose indication that there is no network connection (see Thurrott, for example). This display also reads on the label.

27. As per claim 50-51, the remote server disclosed by Windows 2000 in "Folder and File Encryption On a Remote Server" may also be interpreted as an end user device. Although Windows 2000 does not explicitly disclose a message sent to the end user device instrumental in causing the end user device to preserve the confidentiality of

the sensitive healthcare information an ordinary artisan would readily recognize that in order to encrypt files on the end user device (Remote Server), an appropriate instruction (that would read on a message) would have to be sent to the end user device.

The limitation: "detecting existence of a requirement to preserve confidentiality of the sensitive information" is at least obvious if not inherent. In Windows 2000 it is a user that determines whether confidentiality of the sensitive information is to be preserved and clearly the user must believe that, at least in user's mind, a requirement exists to preserve confidentiality.

28. Finally, Windows 2000 does not disclose that the sensitive information comprises healthcare information. However, the examiner points out that implementing Schmidt's invention into various type of information (e.g. healthcare information) would not affect the functionality of the invention. Additionally, the Official Notice is taken that it is old and well known to store sensitive information that is healthcare information in a memory store (e.g. medical records stored on PCs and/or Servers, e.g. USPub. 2002/0026105, USPub. 2003/0179223, USPub. 2003/0208382 etc.), and it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement Microsoft 2000 invention as disclosed by Microsoft TechNet into healthcare information given the benefit of security.

29. Claims 1-3, 8-10 are rejected under 35 U.S.C. 103(a) as obvious over Blakley (USPN 5677952) in view of Schneier (Bruce Schneier, "Applied Cryptography, Protocols, Algorithms and Source Code in C", 2nd edition, 1996 ISBN: 0471128457).

As per claims 1, 3, 8-9, Blakley discloses an end user device comprising a memory store (36 and/or 35) a data bus connected to the memory store (31) adapted for transporting data to and from the memory store, a processing entity (32) operative to release read and write commands toward the memory store (Fig. 1 and 2, and associated text).

Blakley discloses a device driver that transparently encrypts and decrypts all access to and from the disk using a secret key stored in a volatile memory (Blakley, col. 4 line 64- col. 5 line 19), which reads on an encryption module that is operative to encrypt/decrypt, in accordance with an encryption key, data to be written into/read from the memory store. In order fro data to be written to memory stores computer systems issue write commands. Similarly, read commands are used to read data from memory stores. Also, data written to a memory store would read on first data while data read from memory store would read on second data.

30. Blakley, does not disclose implementation of the encryption module (the device driver) in hardware. Thus, Blakley's disclosure is silent in regard to the encryption module being communicatively coupled to the processing and the data bus. However, hardware implementation of an encryption module is old an well known in the art as illustrated by Schneier (pg. 223-225), and it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement the hardware module disclosed by Blakley given the benefit of speed.

31. As per claim 2, Blakley in view of Schneier do not explicitly disclose the use of a common application specific integrated circuit (ASIC) (e.g. to implement the

processing entity and the encryption module). However, utilizing ASIC would have been an obvious variation that is well known in the art (e.g. NetworkWorld). One would have been motivated to use them especially in light of the benefits of these technologies as evidenced by their commercial success.

32. As per claim 10, Blakley in view of Schneier do not explicitly disclose that the encryption key is the same as the decryption key. However, an ordinary artisan would recognize that in the art of data security there are essentially two types of cryptographic functions: a symmetric and an asymmetric function (e.g. DES and PGP). The symmetric functions use the same key to encrypt and decrypt and it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to utilize the same encryption and decryption key (utilize symmetric cryptography) given the benefit of speed.

33. Claim 38-43 are rejected under 35 U.S.C. 103(a) as obvious over Windows 2000 as illustrated by Microsoft TechNet" (Microsoft TechnNet "Data Protection Implementing the Encrypting File System in Windows 2000" posted in "Windows 2000 File Systems Tutorials", in particular: "Step-by-Step Guide to Encrypting File System (EFS)" article on 05/2002) in view of Blakley (USPN 5677952) and Schneier (Bruce Schneier, "Applied Cryptography, Protocols, Algorithms and Source Code in C", 2nd edition, 1996 ISBN: 0471128457).

As per claim 38, Windows 2000 as illustrated by Microsoft TechNet discloses the end user implementing encryption in order to preserve confidentiality of the sensitive information stored in the memory store as discussed above.

34. TechNet is silent regarding details of the device. Specifically, TechNet does not disclose that the end user device implementing Windows 2000 comprises a data bus connected to the memory store, the data bus being adapted for transporting data to and from the memory store; an encryption module communicatively coupled to the control entity and to the data bus; the control entity being further operative to release read and write commands towards the memory store, the write command being accompanied by first data intended to be written to the memory store; upon the control entity releasing a write command accompanied by said first data, the encryption module being operative to encrypt, in accordance with an encryption key, said first data and send an encrypted version of said first data onto the data bus for writing into the memory store; upon the control entity releasing a read command, the encryption module being operative to decrypt, in accordance with a decryption key, an encrypted version of second data received from the memory store via the data bus and provide said second data to the control entity.

However, these details are disclosed by Blakley in view of Schneier's end user device implementing encryption/decryption, as discussed above. Both of these inventions are concerned with preserving confidentiality of information and both of these inventions use encryption processes to facilitate the confidentiality. Thus, the advantages of the systems of Blakley in view of Schneier and TechNet could have been easily combinable with more than reasonable expectations of success. It would have been obvious to one of ordinary skill in the art at the time of applicant's

invention to implement Blakley in view of Schneier's invention into TechNet invention in order to facilitate the process of information encryption.

35. The limitations of claims 39 and 41 are implicit. End user devices are not limited to a particular user. Thus, an encryption key (as well as corresponding decryption key) would have to be changed in order to ensure true confidentiality. Similarly implicit is limitation of claim 40. Leaving (not deleting) a decryption key violate the principle of data confidentiality because the retrieved decryption key would allow any party to compromise confidentiality of the encrypted information.

36. As per claims 42-43, "the previous decryption key" used prior to use of "the new decryption key" must be stored in memory at the time that process of encryption is taking place in order for the end user device being able to operate on it (the previous decryption key). Similarly, the decryption process (when confidentiality of the sensitive information no longer needs to be preserved) involves (previous) decryption key.

37. Claims 1-14 are rejected under 35 U.S.C. 103(a) as obvious over White (Ron White, "How Computer Work", 7th edition, ISBN: 0789730332, October 2003) in view of Fairclough (USPN 6963979).

As per claims 1, 8-9, White discloses that computer system comprise data bus system enable to communicate data between system's component (pg. 16-17 and 28-29, for example). The system comprises processing entity operative to release read and write commands (CPU, pg. 18, for example) to read write data in a memory store (e.g. Hard Drive, pg. 28 and 29, RAM pg. 17 etc.).

38. White does not disclose an encryption module being operative to encrypt/decrypt data written/read to/from the memory store.

Fairclough discloses an encryption module being operative to encrypt/decrypt data written/read to/from the memory store (e.g. Fig. 1 and col. 2 line 8- col. 3 line 25). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement an encryption module as disclosed by Fairclough given the benefit of data security.

39. As per claims 2-6 and 10-15, Fairclough discloses implementation of a common application-specific integrated circuit (ASIC, col. 4 line 48-49), memory storing encryption and decryption key (Fig. 1, key storage) and use of symmetric keys (col. 4 lines 35-37). Although, Fariclough does not explicitly disclose that the memory storing keys is a volatile memory, col. 1 lines 43-55, for example, clearly discloses that implementation of a volatile memory would have been an obvious variation given the benefit of enable key exchange. Erasing the portion of the volatile memory upon receiving a signal indicating that the key is no longer needed, is implicit: an ordinary artisan in the art of computer security would readily recognize that keeping no longer used keys pose unnecessary security threats.

The examiner considers object 15, in Fig. 1 to read on selection/control module, and as it is clear from Fig. 1, any cryptographic data (keys) handled by the encryption module is received from the selection/control module, and a signal received by the selection/control module indicates the need to exchange data (an encryption state) with the encryption module.

As per claim 7, although Fairclough suggests exchange of encryption keys (col. 1 lines 43-55), Fariclough's disclosure is silent regarding a policy applied in response to stimuli received from a host entity and a user of the data processing apparatus. However, an ordinary artisan would recognize the use of a program/software routine necessary to implement the process of exchange encryption keys. The examiner considers a particular implementation of use of the particular encryption keys (due to communication with a host entity and action of a user of the data processing apparatus) to read on a policy.

Conclusion

Claims 23-33 and 53-55 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Davis (USPN 5818939),

Garfinel (USPN 6993661),

Obara (USPub 2003/0037247),

Pham (USPub 2003/0115447),

Nakamura (USPub 2005/0246553).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571) 272-3840. The examiner can normally be reached Monday through

Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

8/20/07

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER